Windows Server 2012

What's New about Security and Hypervisor

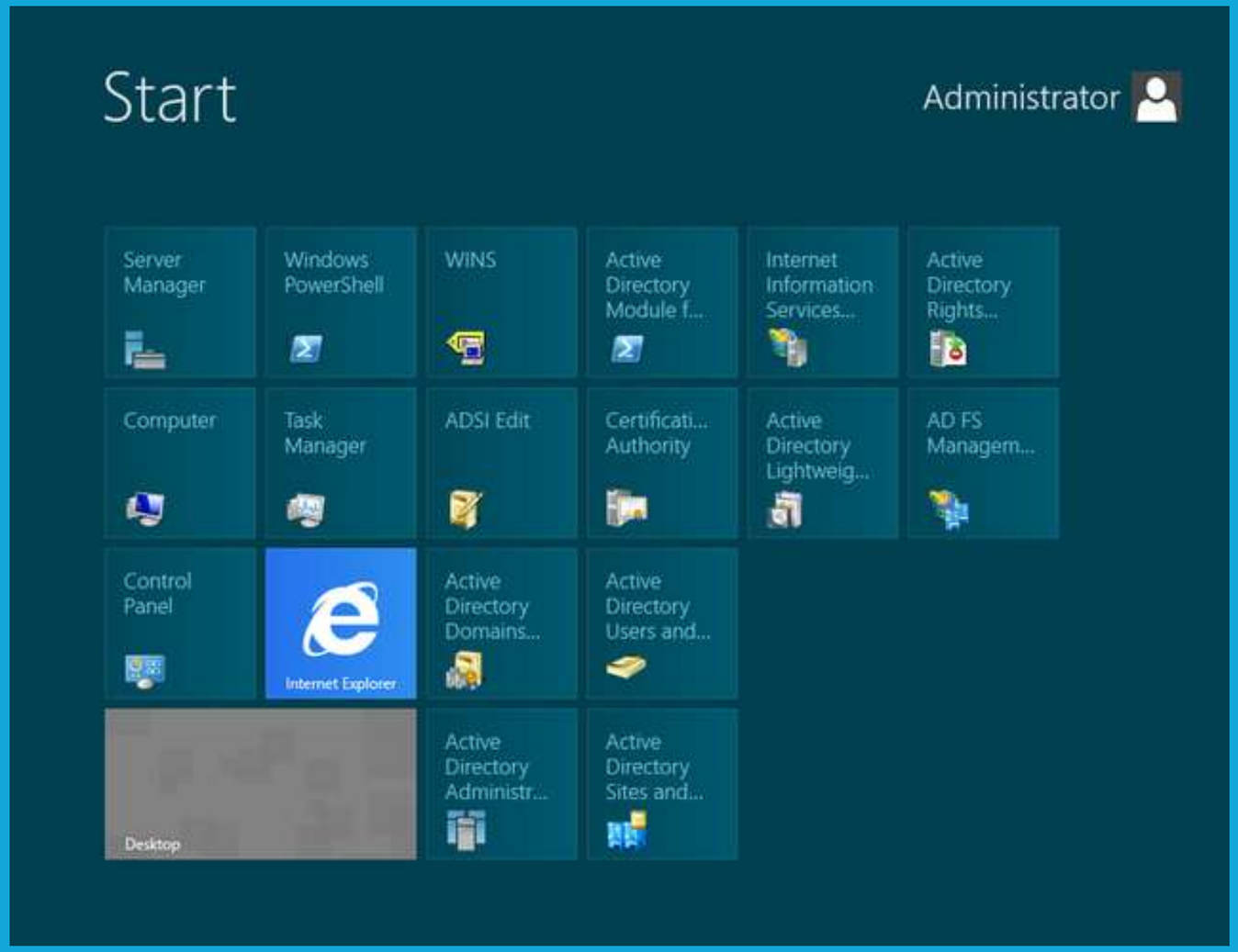
Prinya Hom-anek

CGEIT, CRISC, CISSP, CSSLP, CISA, CISM, CBCI, CFE, SSCP,
ITIL Expert V3, SANS GIAC GCFW, IAPP CIPP Foundation
IRCA: ISMS Lead Auditor, BCMS Auditor

(ISC)2 Asian Advisory Board;
ISACA - Bangkok Chapter Committee, ITSMF Thailand Board,
Thailand Information Security Association (TISA) Committee,
ACIS Professional Center Co., Ltd. , President and Founder

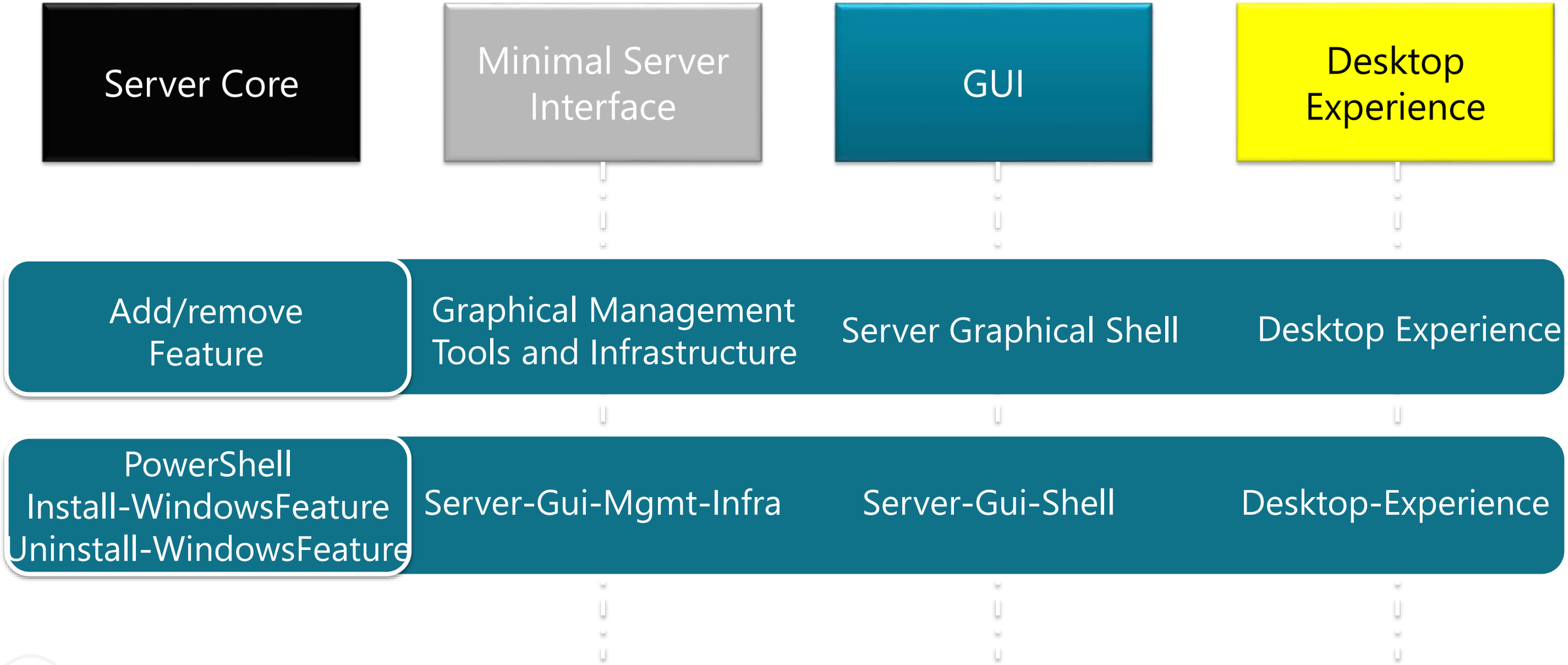
Windows Server 2012

Windows Server 2012 Start Screen

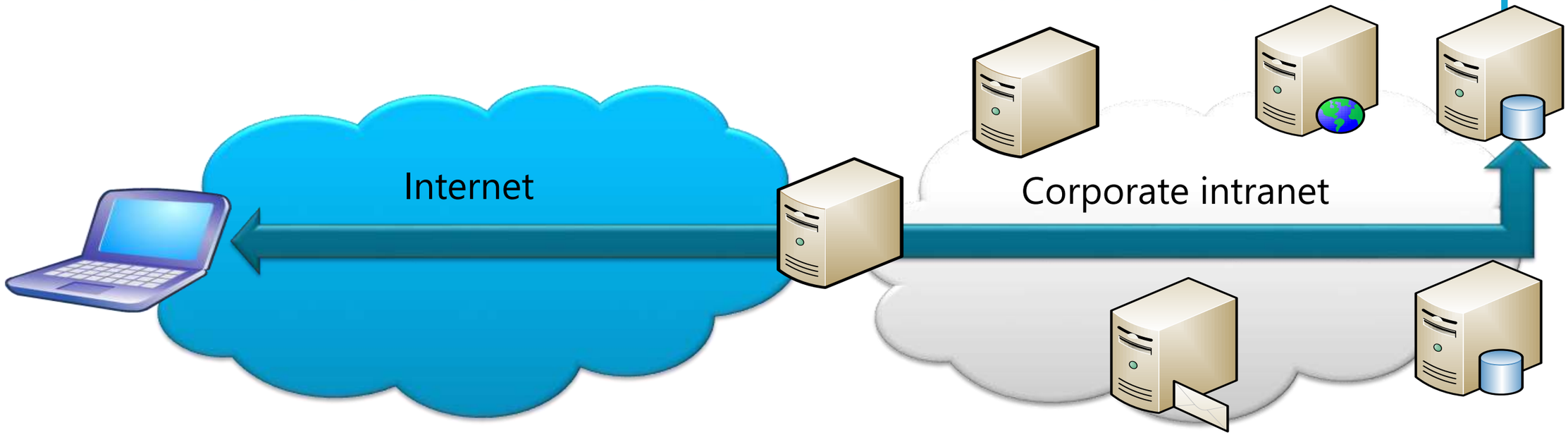


The Microsoft Hybrid Cloud

Easy to switch



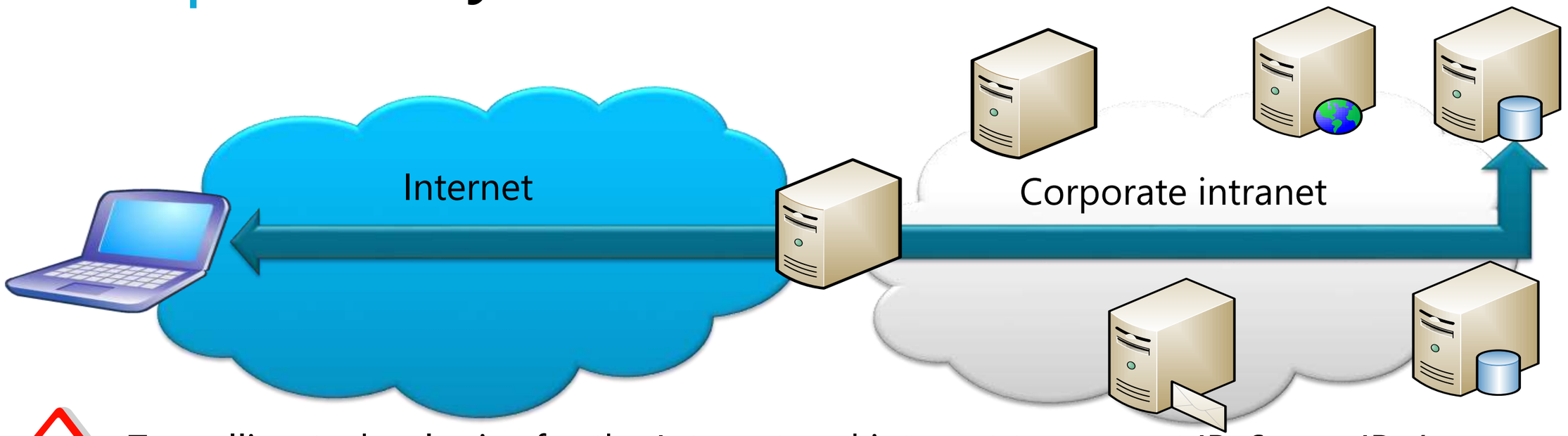
Windows Server 2012 DirectAccess – Simple?



- When a DirectAccess client connects to the Internet it is automatically connected to the corporate intranet
  - No user action required

It’s a truly great user experience - But…

Simple? May Be Not



Tunnelling technologies for the Internet and intranet to support IPv6 over IPv4

Internet tunnelling selection based on client location – Internet, NAT, firewall

Encryption/authentication of Internet traffic (end-to-edge/end-to-end)
PKI required

Client location detection: Internet or corporate intranet

Certificates require PKI

“Building your own cloud just got a lot easier with Windows Server 2012”.

Did you know?

- 9.9 billion messages a day via Windows Live Messenger
- 600 million unique users every month on Windows Live & MSN
- 500 million active Windows Live IDs
- 40M paid MS Online Services (BPOS, CRM online, etc.) in 36 Countries

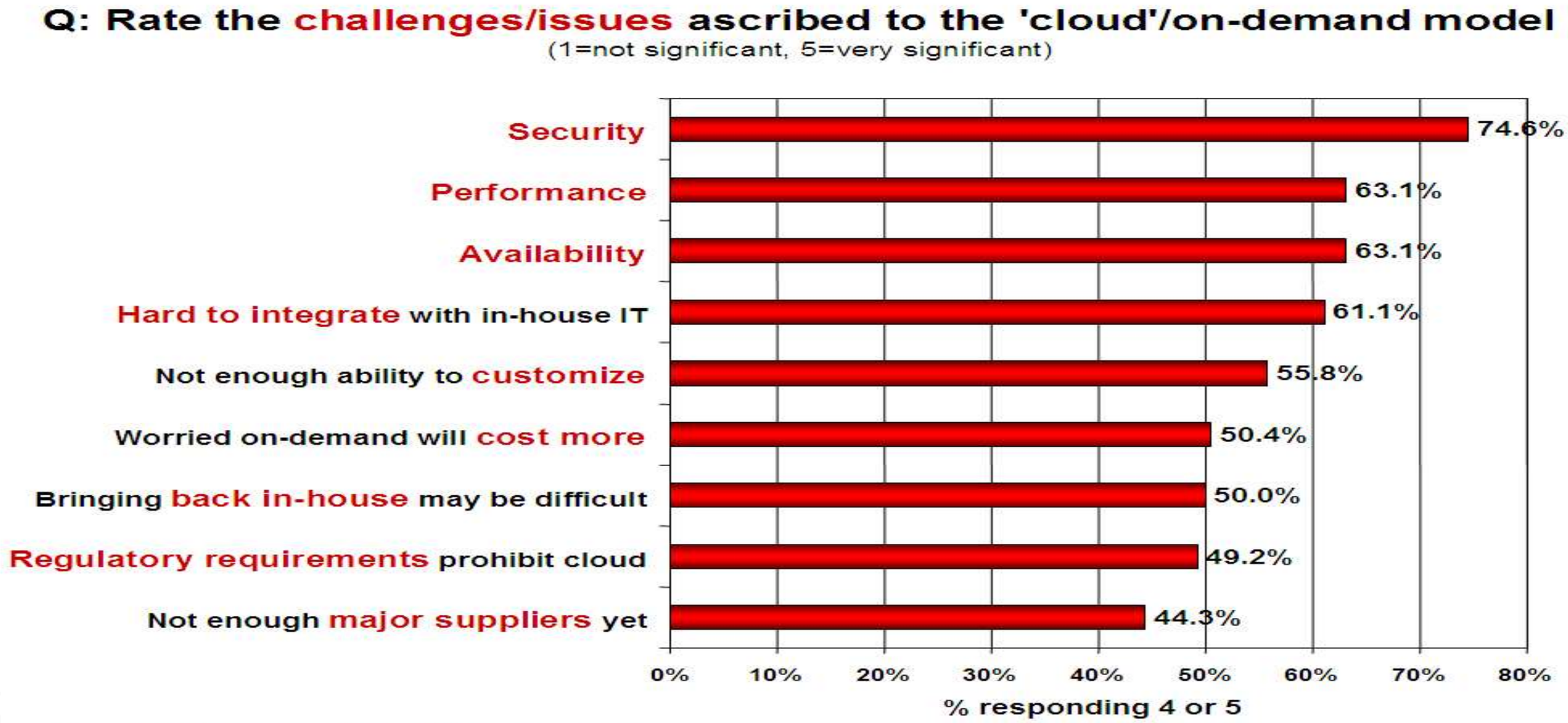
Did you know?

- 5 petabytes of content served by Xbox Live during Christmas week
- 1 Petabyte+ of updates served every month by Windows Update to millions of servers and hundreds of millions of PCs worldwide
- Tens of thousands of Windows Azure customers
- 5M LiveMeeting conference minutes per year
- Forefront for Exchange filters 1B emails per month

Cloud Considerations

- Mission Critical, Scale Up Workloads
- Storage
  - Costs
  - Complexity
  - Security
- Continuous Availability
- VM Mobility
- Networking
  - Multi-Tenancy, Security
  - IP Address Management
  - QoS
- Automation/Manageability

Security is the Major Issue



Source: IDC Enterprise Panel, August 2008 n=244

cloud security alliance℠

CSA https://wiki.cloudsecurityalliance.org/guidance/index.php/Main_Page
CSA Main Page - Security Guida...
Find: presentat Previous Next Options

CSA cloud security alliance

navigation
- Main page
- Community portal
- Current events
- Recent changes
- Random page
- Help

search
Go Search

toolbox
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link

Main Page

Security Guidance for Critical Areas of Focus in Cloud Computing

- Introduction
- Foreword
- Letter from the Editors
- An Editorial Note on Risk
- Section I. Cloud Architecture
  - Domain 1: Cloud Computing Architectural Framework
- Section II. Governing in the Cloud
  - Domain 2: Governance and Enterprise Risk Management
  - Domain 3: Legal and Electronic Discovery
  - Domain 4: Compliance and Audit
  - Domain 5: Information Lifecycle Management
  - Domain 6: Portability and Interoperability
- Section III. Operating in the Cloud
  - Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
  - Domain 8: Data Center Operations
  - Domain 9: Incident Response, Notification, and Remediation
  - Domain 10: Application Security
  - Domain 11: Encryption and Key Management
  - Domain 12: Identity and Access Management
  - Domain 13: Virtualization
- References

Top Threats
to
Cloud Computing V1.0

Prepared by the
Cloud Security Alliance
March 2010

Threat #1: Abuse and Nefarious Use of Cloud Computing .....
Threat #2: Insecure Interfaces and APIs .....
Threat #3: Malicious Insiders.....
Threat #4: Shared Technology Issues .....
Threat #5: Data Loss or Leakage .....
Threat #6: Account or Service Hijacking.....
Threat #7: Unknown Risk Profile .....

- Source : Cloud Security Alliance

So You're a Building a Cloud...

I have good processes in place, but what other safeguards can I use to protect my data?

Server Hard Disks Appear on eBay

Real Case : A US Power Company

- The Company ***had processes in place*** to either physically destroy drives or scrub them to U.S. DOD standards

  - Degaussing

  - Overwriting the data with a minimum of three specified patterns

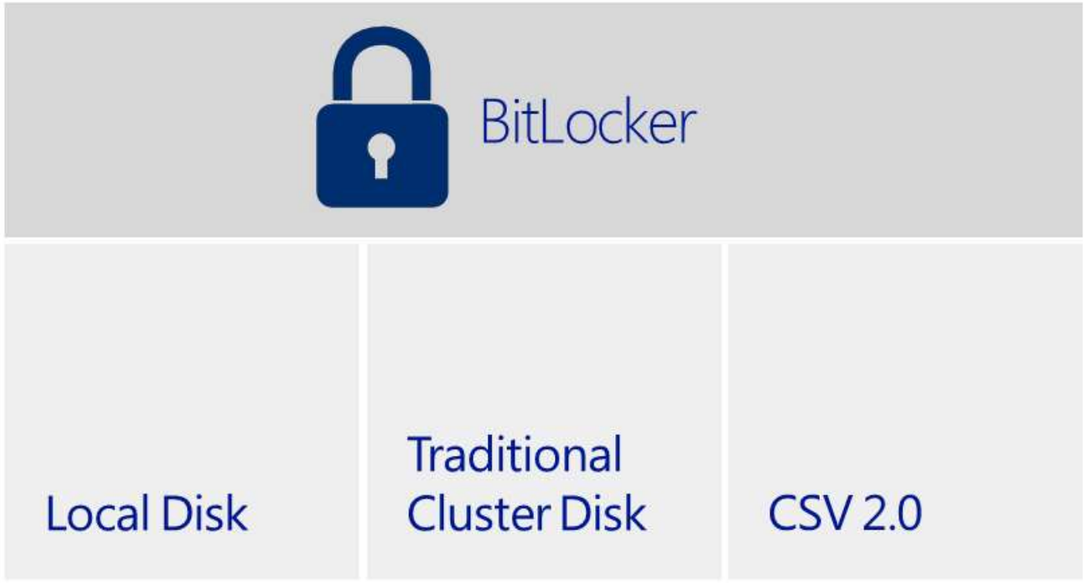
- Data on drives used in servers, contained:

  Proprietary company information such as memos, correspondence

  Customers data (460,000+) & Confidential employee information

According to Gartner about 1/3 companies use outside firms to dispose of PCs & Servers

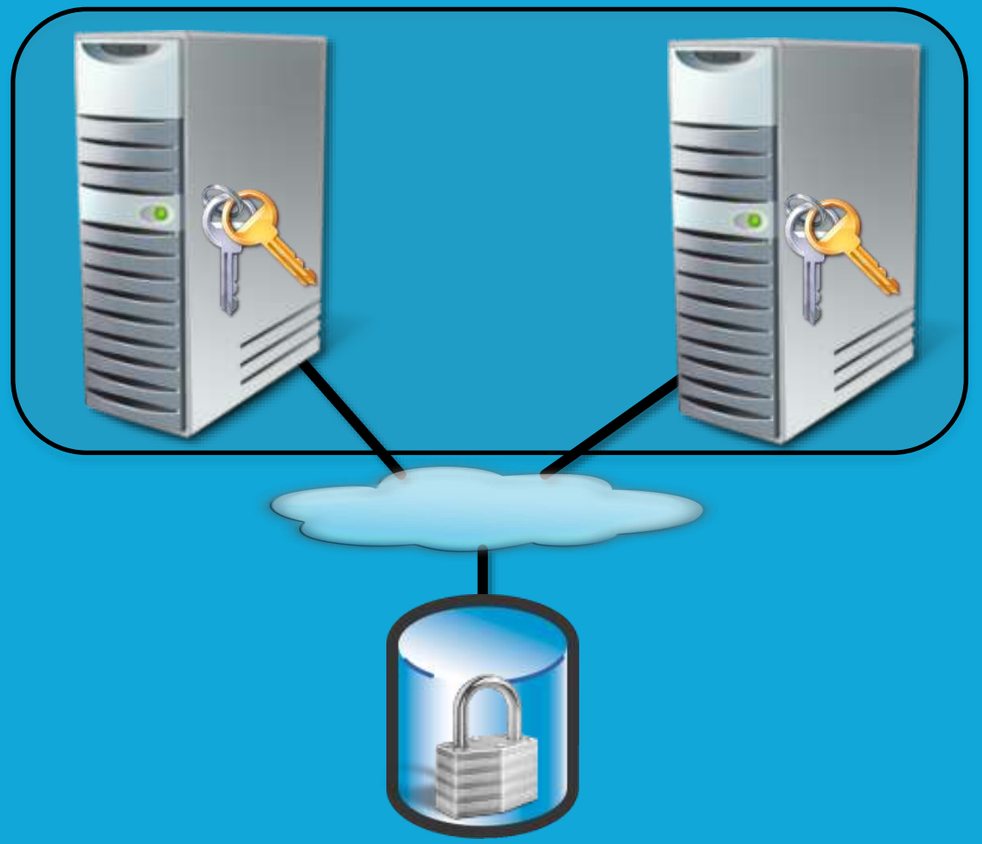
Physical Security



BitLocker ensures your **data stays secure**, even when your Hyper-V hosts, clusters, and storage reside in less-physically-secure locations

Critical Safeguard for the Cloud
Encrypted cluster volumes

- BitLocker encrypted cluster disks
  - Support for traditional failover disks
  - Support for Cluster Shared Volumes
- Cluster Name Object (CNO) identity used to lock and unlock Clustered volumes
- Enables physical security for deployments outside of secure datacenters
  - Branch office deployments
- Volume level encryption for compliance requirements
- Negligible (<1%) performance impact



What's New In Windows Server 2012 Hyper-V

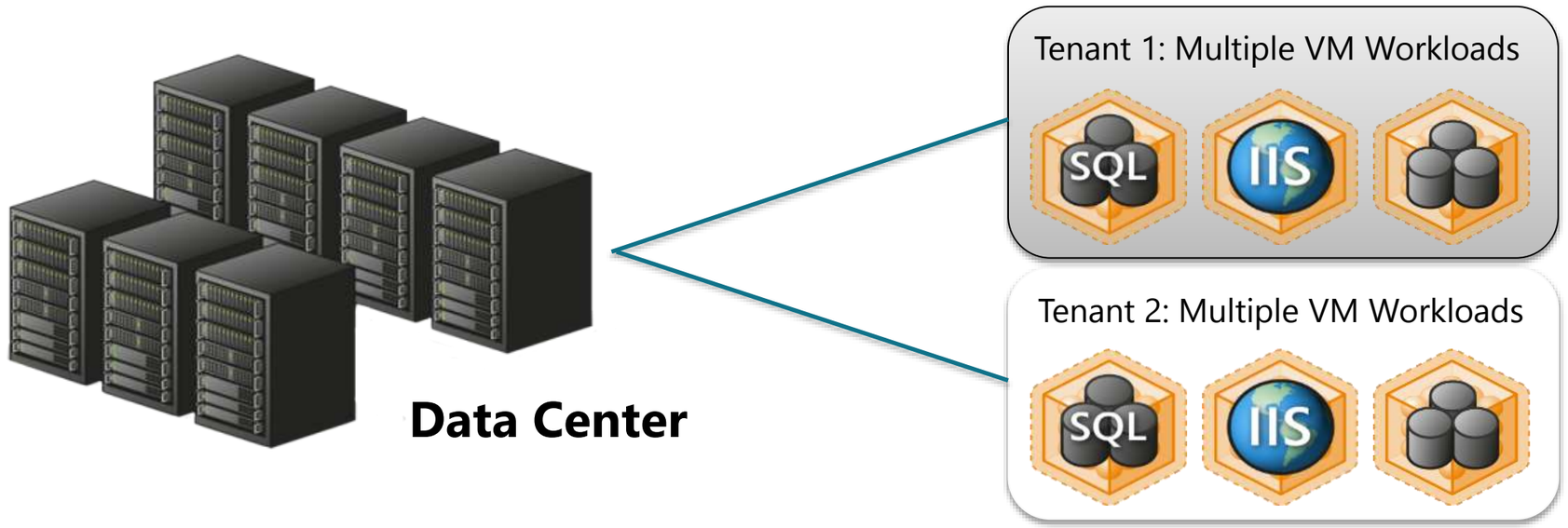
- Scale Up Workloads
- Platform Resiliency
- Storage
- Automation/Manageability
- Networking
- Clustering
- VM Mobility
- Linux as a Guest

Network Considerations

- How do I ensure network multi-tenancy?
- IP Address Management (IPAM) is a pain.
- What if VMs are competing for bandwidth?
- Fully Leverage Network Fabric
- How do I integrate with existing fabric?
- Network Metering?
- Can I dedicate a NIC to a workload?

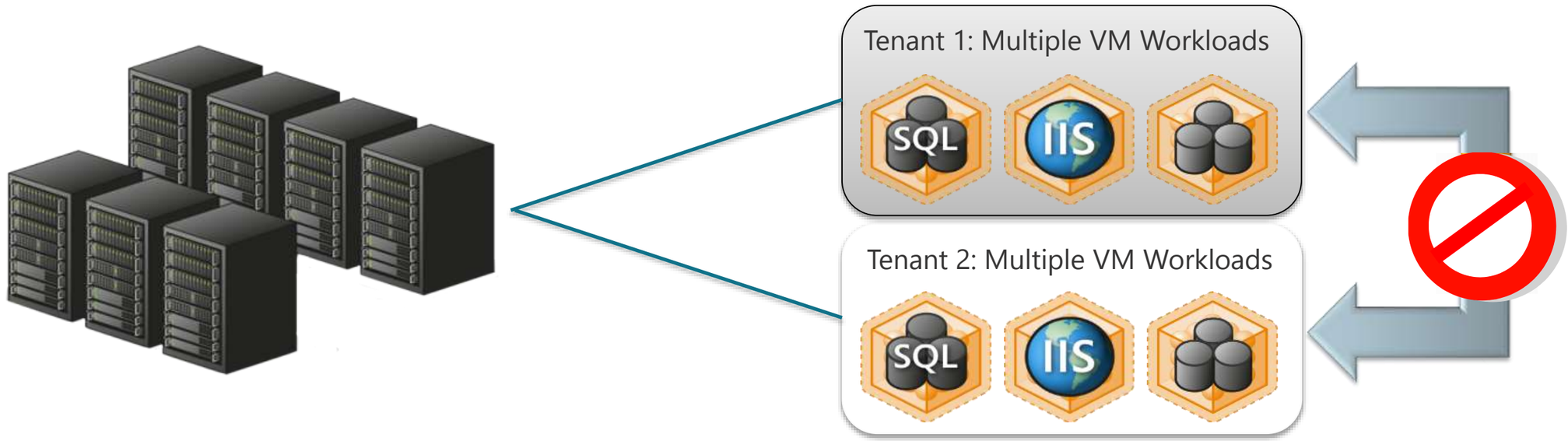
Hybrid Clouds

Windows Server 2012 is optimized for Hybrid Clouds to host multi-tenant workloads



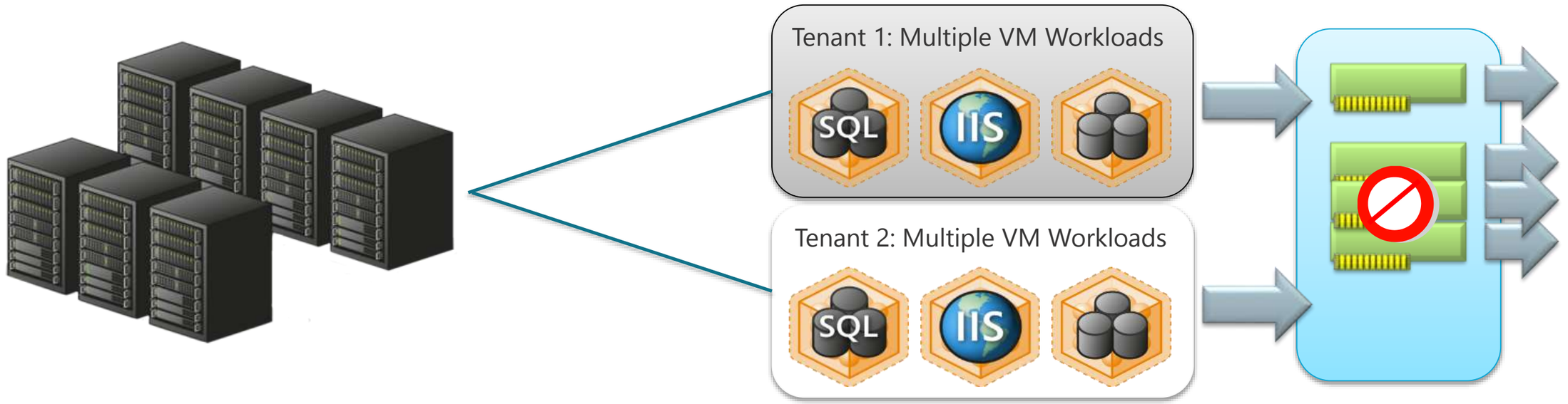
Security

In a multi-tenant environment …
… customers want security and isolation



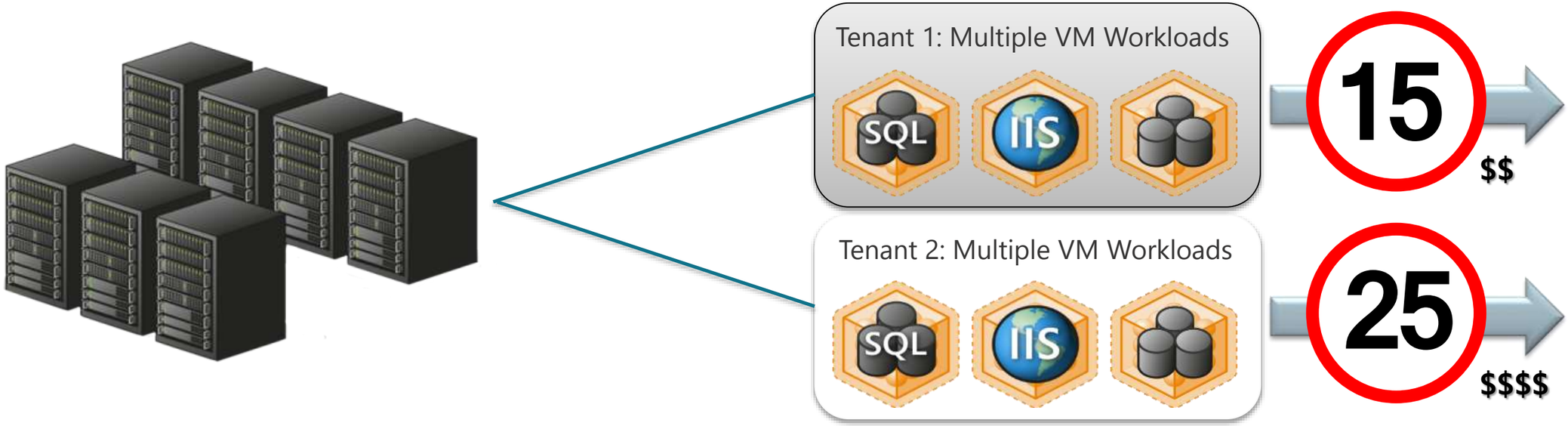
Reliability

Even when hardware fails …
… customers want continuous availability



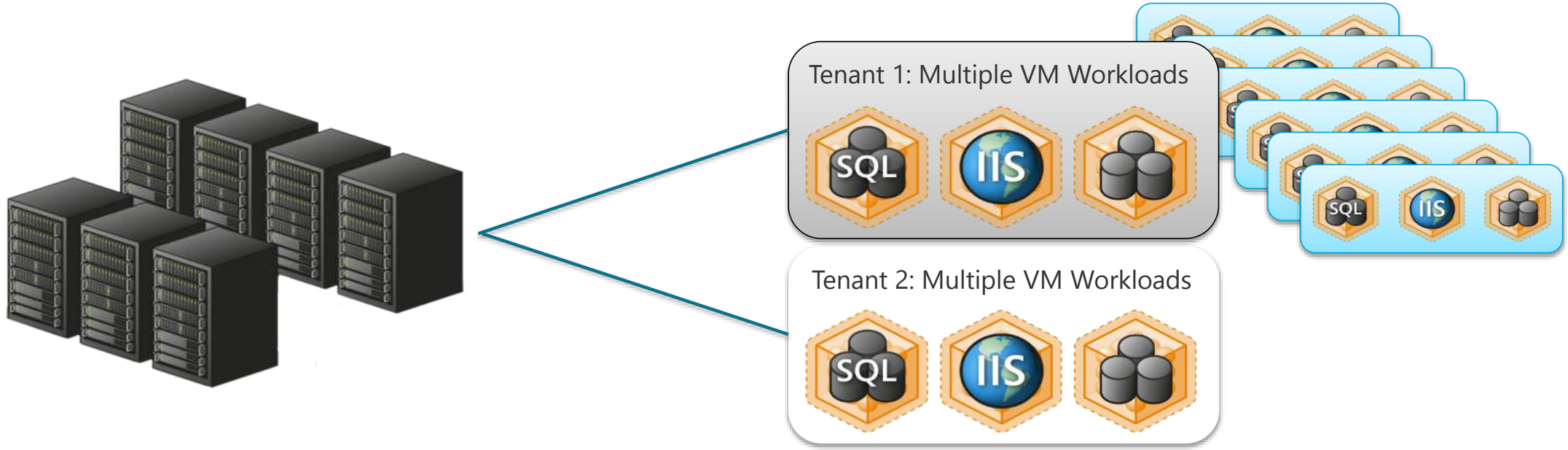
Predictability

Even when multiple VMs are competing for bandwidth …
… customers want predictability



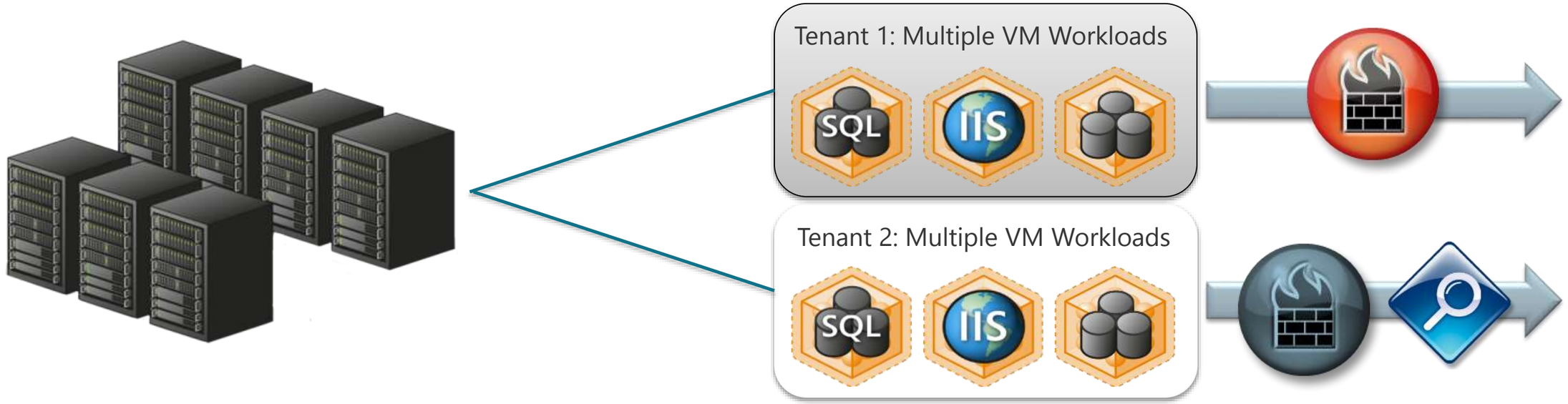
Scalability

Cloud admins want scalability …
… and customers want performance



Extensibility

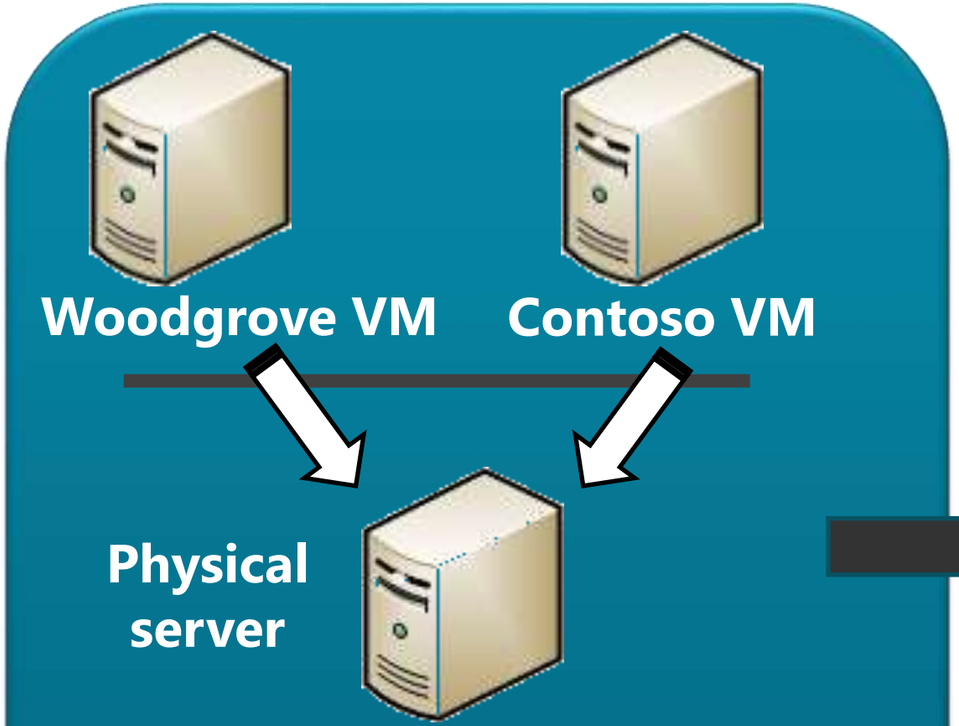
Customers want specialized functionality with lots of choice …
… for firewalls, monitoring and physical fabric integration



Multi-Tenant Network Requirements

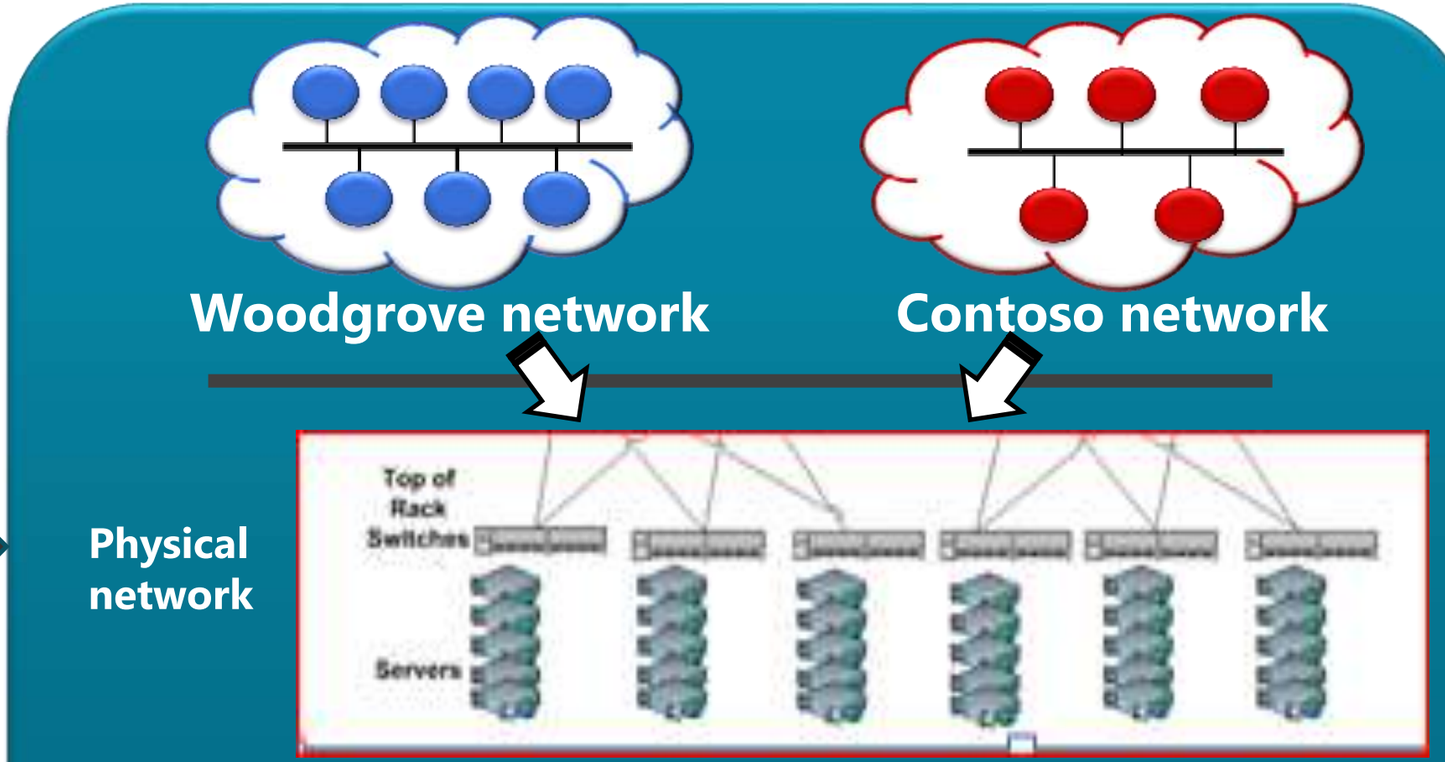
- Tenant wants to easily move VMs to/from the cloud
- Hoster wants to place VMs anywhere in the data center
- Both want: Easy Onboarding, Flexibility & Isolation

Introducing Hyper-V Network Virtualization



Hyper-V Machine Virtualization

- Run multiple virtual servers on a physical server
- Each VM has illusion it is running as a physical server

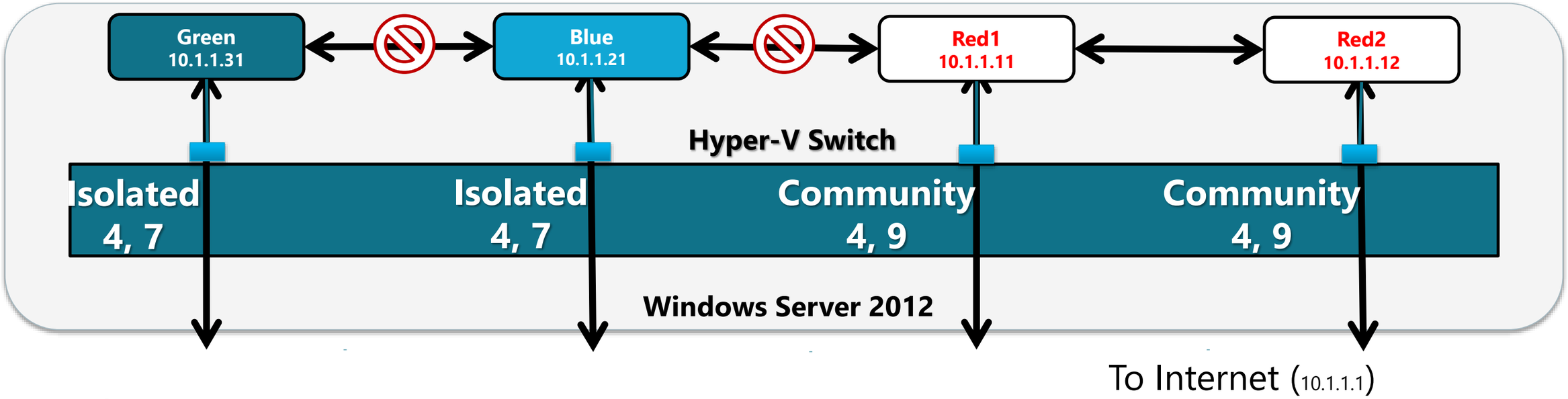


Hyper-V Network Virtualization

- Run multiple virtual networks on a physical network
- Each virtual network has illusion it is running as a physical fabric

[VI305] Hyper-V Network Virtualization for Multi-Tenancy in WS2012

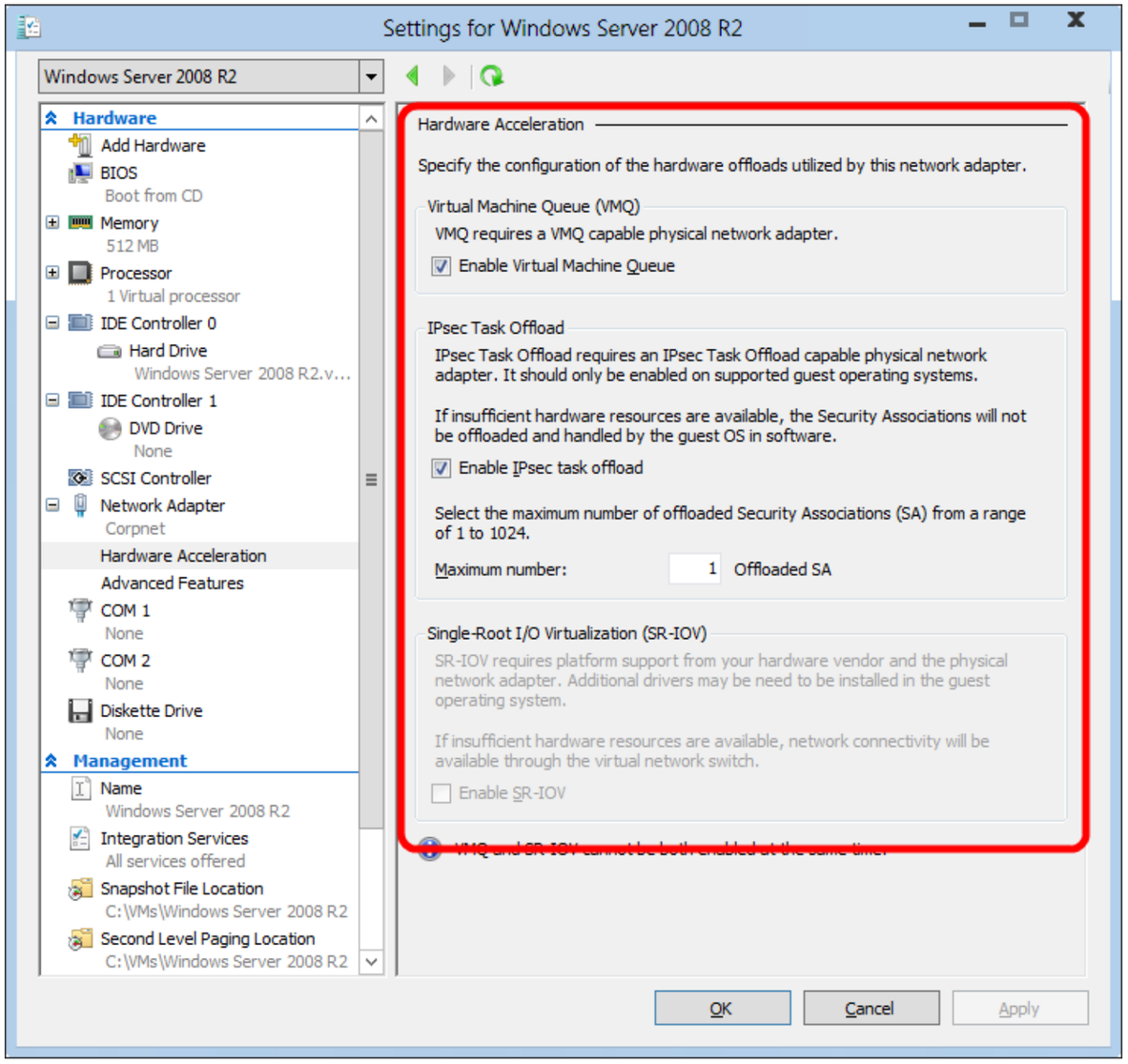
One Solution: PVLAN (Private VLAN)



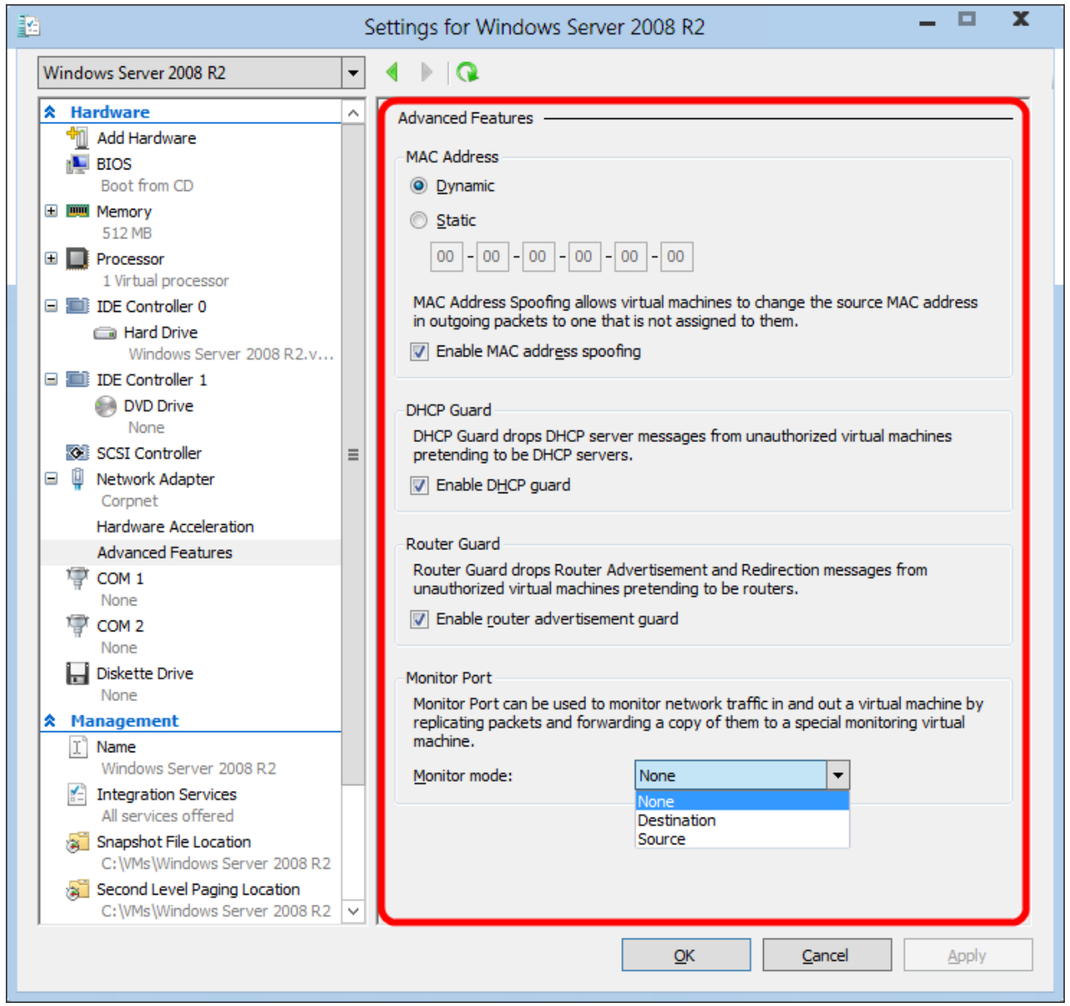
- Isolation Scenario
  - Hoster wants to isolate all VMs from each other and allow internet connectivity
  - #1 Customer Ask from hosters
- Community Scenario
  - Hoster wants tenant VMs to interact with each other but not with other tenant VMs
  - Requires a VLAN id for each “community” (limited scalability, only 4095 VLAN IDs)

Cloud Admins Want Scale, Customers Perf

DVMQ, IPsec Task Offload, SR-IOV

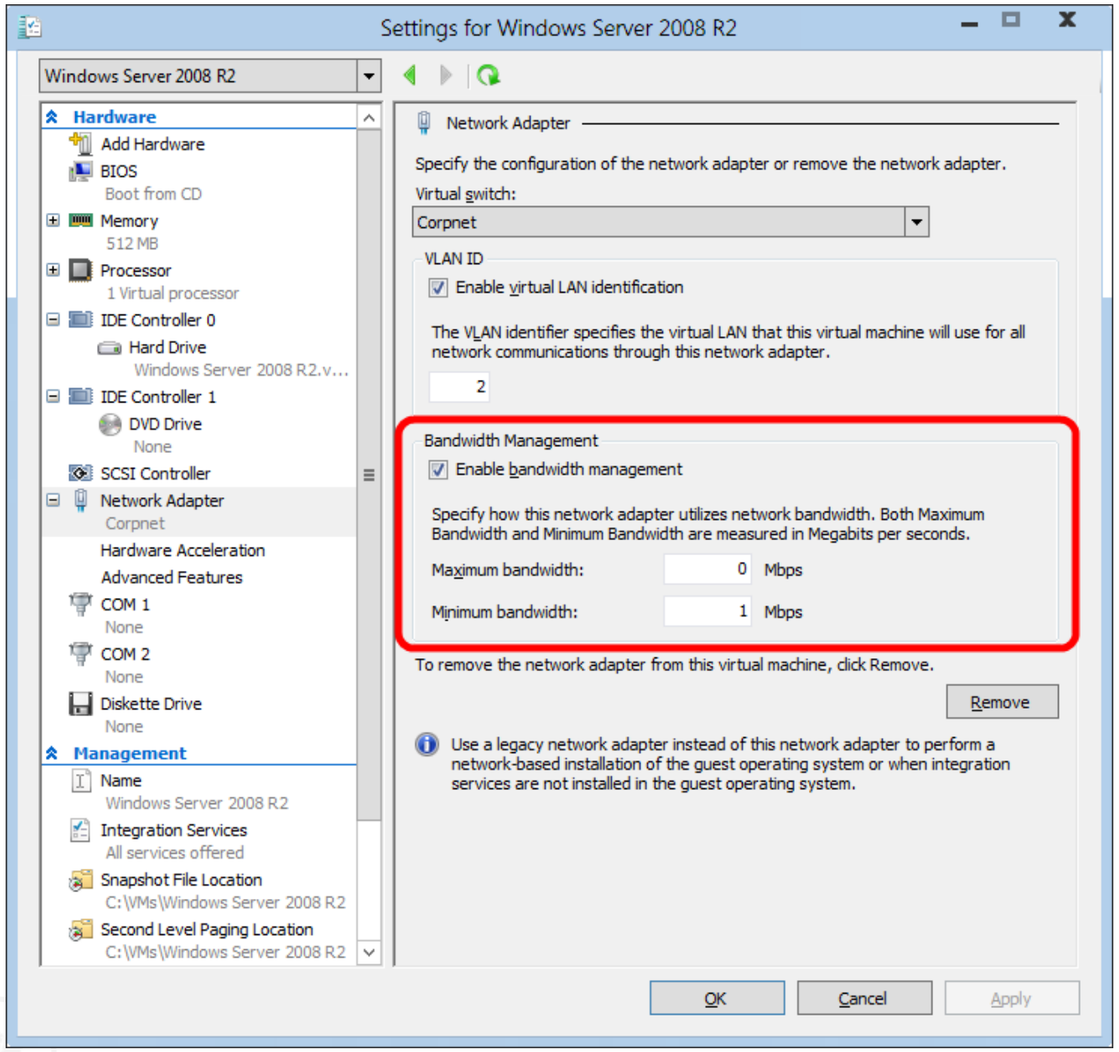

Settings for Windows Server 2008 R2
Windows Server 2008 R2
Hardware
Add Hardware
BIOS
Boot from CD
Memory
512 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
Windows Server 2008 R2.v...
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
Corpnet
Hardware Acceleration
Advanced Features
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
Windows Server 2008 R2
Integration Services
All services offered
Snapshot File Location
C:\VMs\Windows Server 2008 R2
Second Level Paging Location
C:\VMs\Windows Server 2008 R2
Hardware Acceleration
Specify the configuration of the hardware offloads utilized by this network adapter.
Virtual Machine Queue (VMQ)
VMQ requires a VMQ capable physical network adapter.
Enable Virtual Machine Queue
IPsec Task Offload
IPsec Task Offload requires an IPsec Task Offload capable physical network adapter. It should only be enabled on supported guest operating systems.
If insufficient hardware resources are available, the Security Associations will not be offloaded and handled by the guest OS in software.
Enable IPsec task offload
Select the maximum number of offloaded Security Associations (SA) from a range of 1 to 1024.
Maximum number:
1
Offloaded SA
Single-Root I/O Virtualization (SR-IOV)
SR-IOV requires platform support from your hardware vendor and the physical network adapter. Additional drivers may be need to be installed in the guest operating system.
If insufficient hardware resources are available, network connectivity will be available through the virtual network switch.
Enable SR-IOV
OK
Cancel
Apply

Advanced Network Security
DHCP Guard, Router Guard, Monitor Port



- **DHCP Guard** is a security feature that drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.
- **Router Guard** is a security feature that drops Router Advertisement and Redirection messages from unauthorized virtual machines pretending to be routers.
- **Monitor Mode** duplicates all egress and ingress traffic to/from one or more switch ports (being monitored) to another switch port (performing monitoring)

Manage to a Service Level Agreement
Network Bandwidth & QoS



- **Bandwidth Management** allows you to easily reserve minimum or set maximums to provide QoS controls to manage to a service level agreement

Windows Server 2012 Networking: It's All There

	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012
NIC Teaming	Yes, via partners	Yes, via partners	Windows NIC Teaming in box.
VLAN Tagging	Yes	Yes	Yes
MAC Spoofing Protection	No	Yes, with R2 SP1	Yes
ARP Spoofing Protection	No	Yes, with R2 SP1	Yes
SR-IOV Networking	No	No	Yes
Network QoS	No	No	Yes
Network Metering	No	No	Yes
Network Monitor Modes	No	No	Yes
IPsec Task Offload	No	No	Yes
VM Trunk Mode	No	No	Yes

Beyond Virtualization

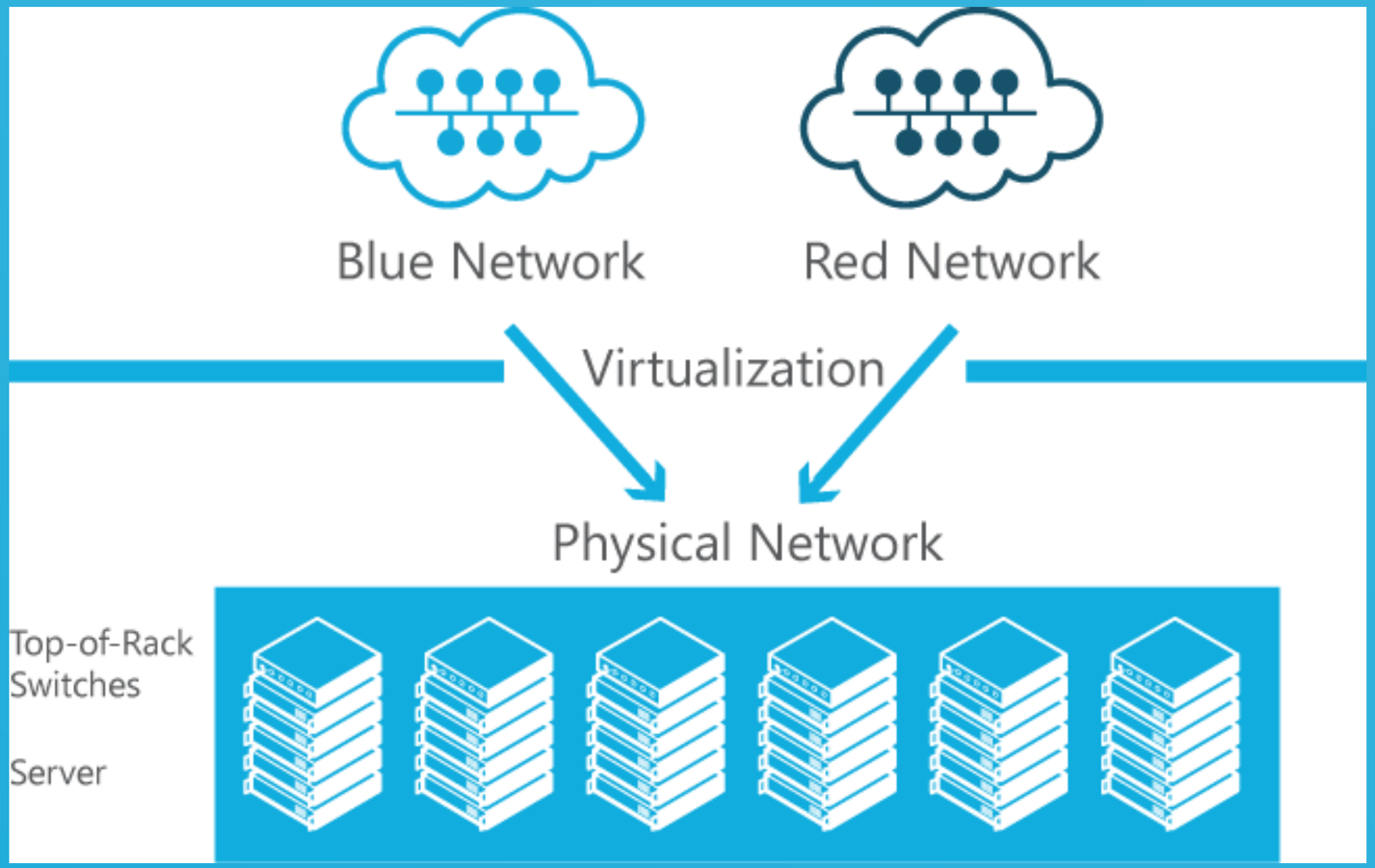
Complete Virtualization Platform

Delivering a fully isolated, multitenant environment that includes tools to guarantee SLAs, enable chargebacks, and support self-service delivery

- **Multitenant security and isolation**: Secure separation of resources in the data center as needed per host
- **Hyper-V Network Virtualization**: Scale beyond VLANs by moving workloads without changing network configurations or reconfiguring physical networks
- **Extensible Switch**: Inspect, forward or report on traffic in the virtual environment based on needs
- **Quality of Service**: Guarantee minimum services bandwidth while maximizing network throughput

Complete Virtualization Platform

Scale beyond VLANs with Hyper-V Network Virtualization

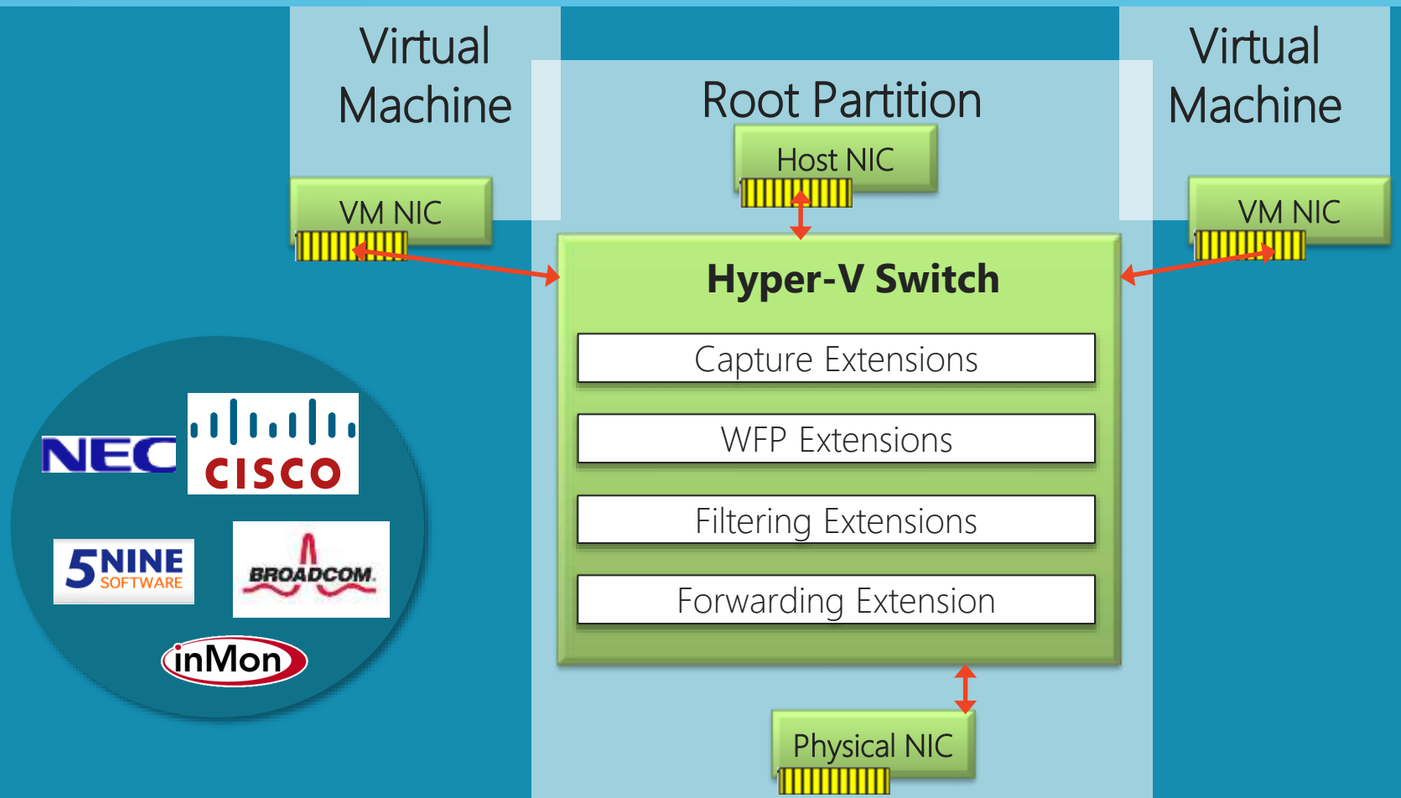


Run multiple virtual networks on a single physical network. Each virtual network believes it is running on its own physical fabric.

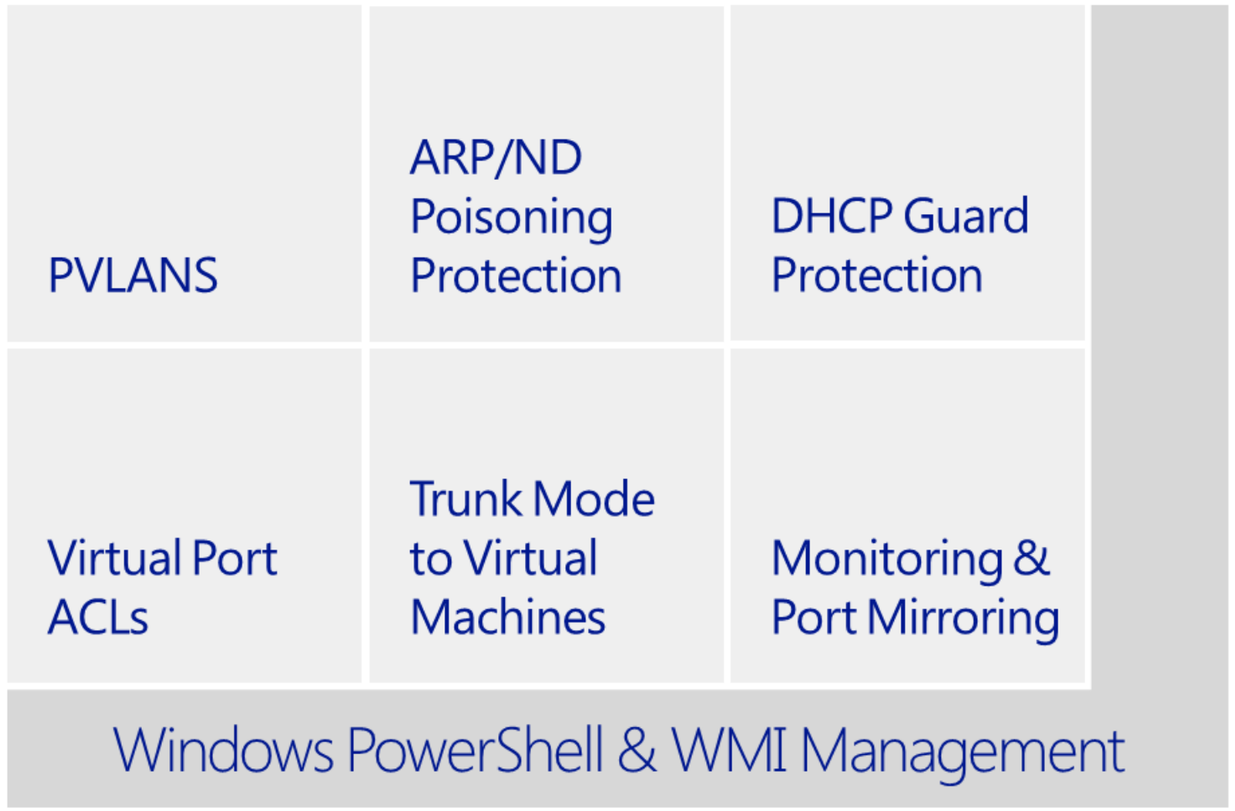
Beyond Virtualization

Hyper-V Extensible Switch

Augmented Hyper-V Virtual Switch capabilities, offering monitoring, traffic filtering & shaping, and forwarding algorithms



Hyper-V Extensible Switch

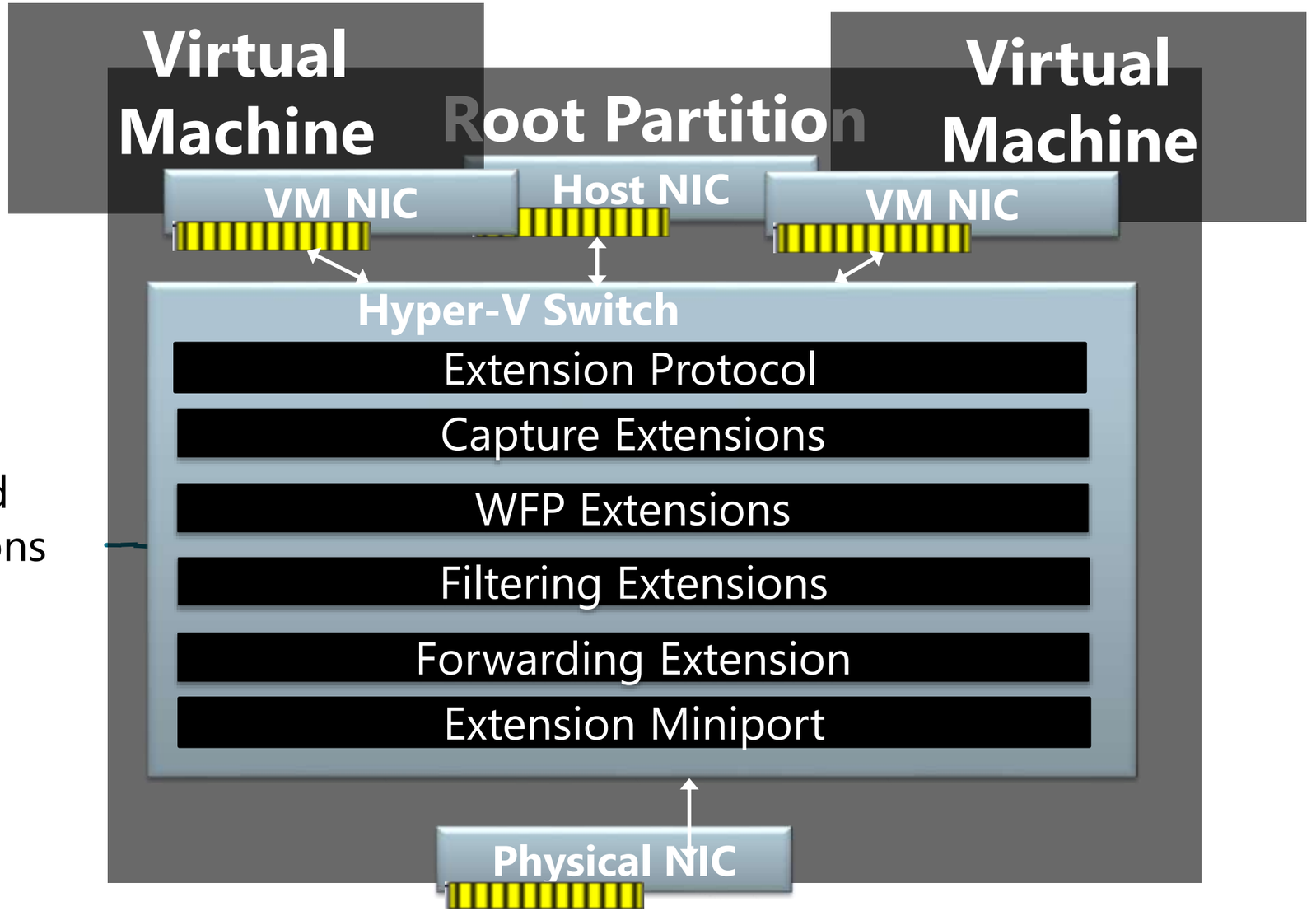


The Hyper-V Extensible Switch allows a **deeper integration** with customers' existing network infrastructure, monitoring and security tools

Hyper-V Extensible Switch

Hyper-V Extensible Switch is an open platform that lets **multiple** vendors provide extensions that are written to standard Windows API frameworks

Hyper-V Extensible Switch



Partners and Their Extensions

- sFlow traffic (capture)
- Virtual Firewall v3.0 (filtering)
- Nexus 1000V (forwarding)
- UCS (forwarding w/SR-IOV)
- OpenFlow (forwarding)

CISCO

NEC

Networking Performance

Dynamic VMq	Dynamically span multiple CPUs when processing virtual machine network traffic
IPsec Task Offload	Offload IPsec processing from within virtual machine, to physical network adaptor, enhancing performance
SR-IOV Support	Map virtual function of an SR-IOV capable physical network adaptor, directly to a virtual machine

The Hyper-V Extensible Switch takes advantage of hardware innovation to drive the **highest levels of networking performance** within virtual machines

Network Virtualization

Secure Isolation

Isolate network traffic from different business units or customers on a shared infrastructure without VLANs

Flexible Migrations

Move VMs as needed within your virtual infrastructure while preserving their virtual network assignments

Seamless Integration

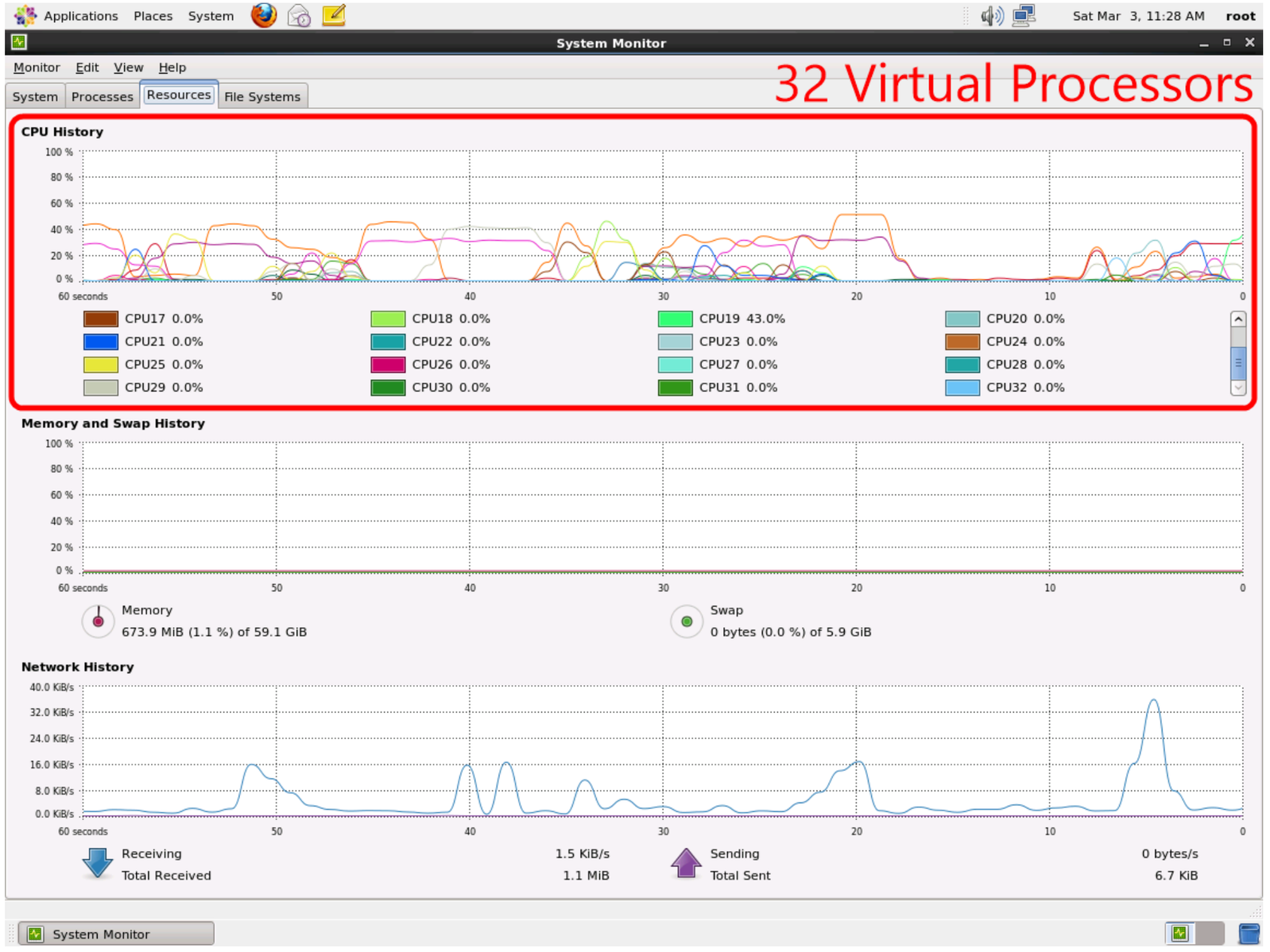
Transparently integrate these private networks into a preexisting infrastructure on another site

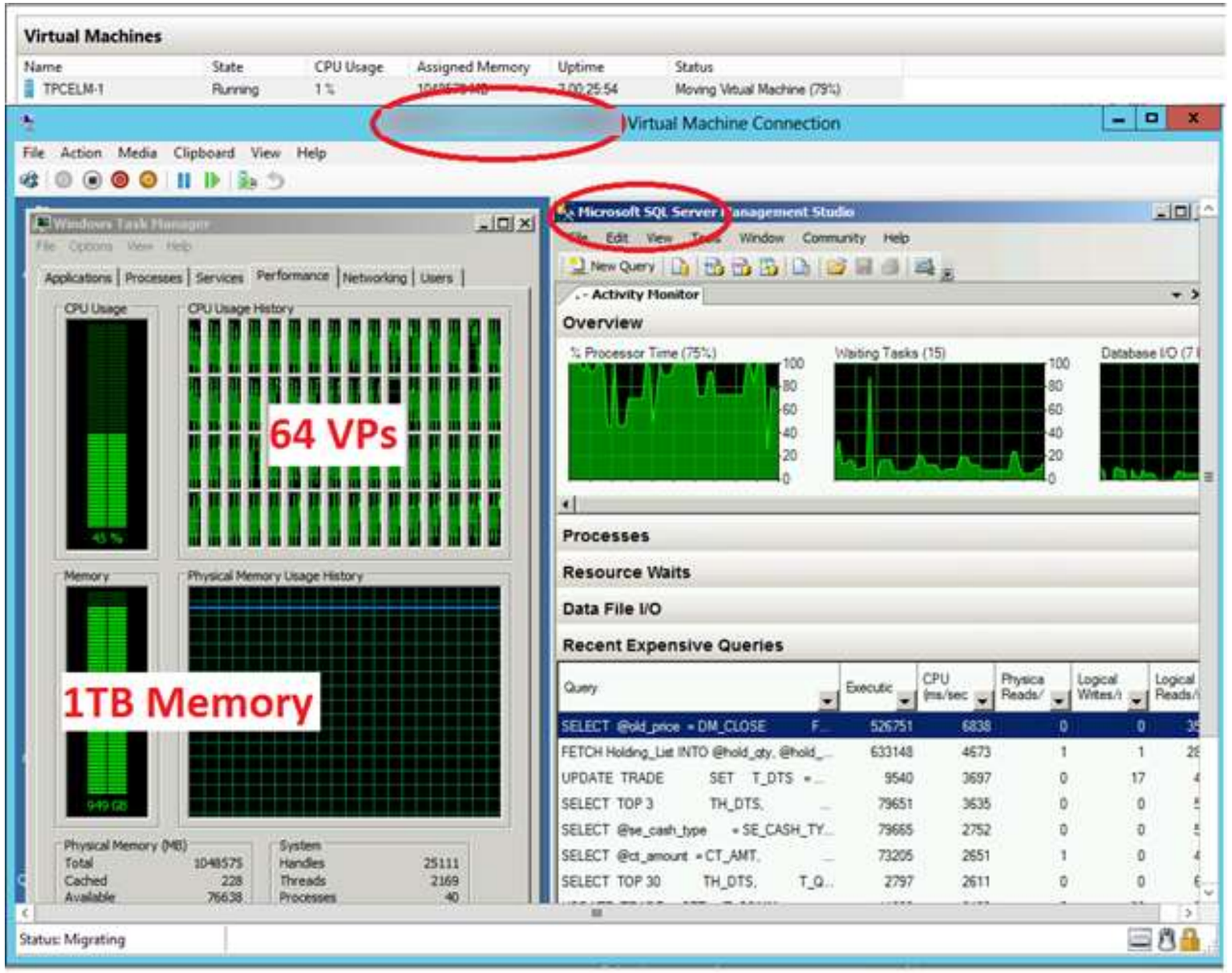
Hyper-V Scalability Improvements

System	Resource	Windows Server 2008 R2 Hyper-V	Windows Server 2012 Hyper-V	Improvement Factor
Host	Logical Processors	64	320	**5×**
	Physical Memory	1TB	4TB	**4×**
	Virtual CPUs per Host	512	2,048	**4×**
VM	Virtual CPUs per VM	4	64	**16×**
	Memory per VM	64GB	1TB	**16×**
	Active VMs per Host	384	1,024	**2.7×**
	Guest NUMA	No	Yes	**-**
Cluster	Maximum Nodes	16	64	**4×**
	Maximum VMs	1,000	4,000	**4×**

"Nothing from Microsoft, and I mean literally **nothing** has ever been this ambitious"

— Jason Perlow, **ZD**Net


Applications
Places
System
Sat Mar 3, 11:28 AM
root
System Monitor
Monitor
Edit
View
Help
32 Virtual Processors
System
Processes
Resources
File Systems
CPU History
100 %
80 %
60 %
40 %
20 %
0 %
60 seconds
50
40
30
20
10
0
CPU17 0.0%
CPU18 0.0%
CPU19 43.0%
CPU20 0.0%
CPU21 0.0%
CPU22 0.0%
CPU23 0.0%
CPU24 0.0%
CPU25 0.0%
CPU26 0.0%
CPU27 0.0%
CPU28 0.0%
CPU29 0.0%
CPU30 0.0%
CPU31 0.0%
CPU32 0.0%
Memory and Swap History
Memory
673.9 MiB (1.1 %) of 59.1 GiB
Swap
0 bytes (0.0 %) of 5.9 GiB
Network History
40.0 KiB/s
32.0 KiB/s
24.0 KiB/s
16.0 KiB/s
8.0 KiB/s
0.0 KiB/s
Receiving
1.5 KiB/s
Total Received
1.1 MiB
Sending
0 bytes/s
Total Sent
6.7 KiB
System Monitor


Virtual Machines
Name
State
CPU Usage
Assigned Memory
Uptime
Status
TPCELM-1
Running
1 %
3.00:25:54
Moving Virtual Machine (79%)
Virtual Machine Connection
File Action Media Clipboard View Help
Windows Task Manager
Applications Processes Services Performance Networking Users
CPU Usage
CPU Usage History
64 VPs
Memory
Physical Memory Usage History
1TB Memory
Physical Memory (MB)
Total 1048575
Cached 228
Available 76638
System
Handles 25111
Threads 2169
Processes 40
Microsoft SQL Server Management Studio
File Edit View Tools Window Community Help
New Query
Activity Monitor
Overview
% Processor Time (75%)
Waiting Tasks (15)
Database I/O
Processes
Resource Waits
Data File I/O
Recent Expensive Queries
Query
Executic
CPU (ms/sec
Physica Reads/
Logical Writes/
Logical Reads/
SELECT @old_price = DM_CLOSE F... 526751 6838 0 0
FETCH Holding_List INTO @hold_qty, @hold_... 633148 4673 1 1
UPDATE TRADE SET T_DTS = ... 9540 3697 0 17
SELECT TOP 3 TH_DTS, ... 79651 3635 0 0
SELECT @se_cash_type = SE_CASH_TY... 79665 2752 0 0
SELECT @ct_amount = CT_AMT, ... 73205 2651 1 0
SELECT TOP 30 TH_DTS, T_Q... 2797 2611 0 0
Status: Migrating

Capability	Windows Server 2012 Hyper-V
Extensible vSwitch	**Yes**
Confirmed Partner Extensions	**4**
Private Virtual LAN (PVLAN)	**Yes**
ARP Spoofing Protection	**Yes**
DHCP Snooping Protection	**Yes**
Virtual Port ACLs	**Yes**
Trunk Mode to Virtual Machines	**Yes**
Port Monitoring	**Yes**
Port Mirroring	**Yes**

Secure Multitenancy

The Availability of Many Servers,
The Simplicity of One

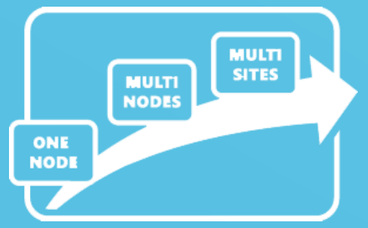
Management Efficiency

Broader automation of common management tasks and a path toward full lights-out automation

- **Multi-server management with Server Manager**: Simplify the processes of configuring new servers, deploying roles and features to Windows Server and managing multiple-server environments
- **Resilient and simple automation with PowerShell**: Expanded cmdlet scope, simplified usage, automation and workflow to manage every aspect of your data center
- **Volume License Activation:** Machines can seamlessly activate when joined to the domain with no additional deployment or configuration requirements

Full automation for all
Workloads and roles

PowerShell 3.0



2,400+ commandlets along with workflows and comsdks;lad;lsakd;lsakdlsad;sakds

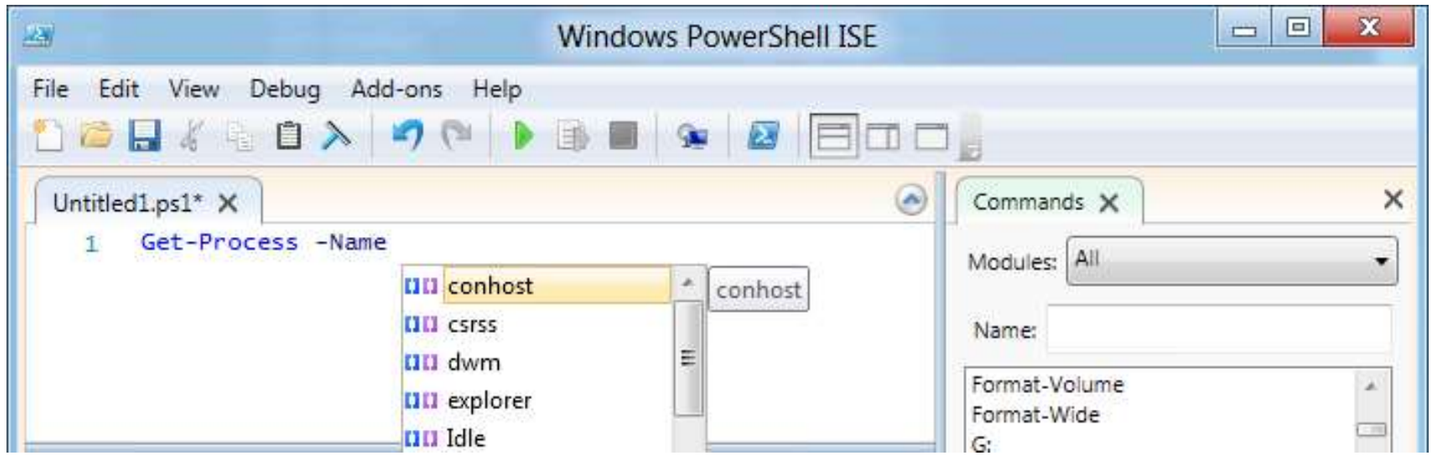
- **Integration for all roles:** New support for SMB, NIC Teaming and Hyper-V management and configuration
- **RunAs Flexibility**: commands may be executed using delegated credentials, allowing limited permission users to run critical jobs
- **Constrained Mode “sandboxes”:** PowerShell cmdlets can restrict access and execution of commands with security implications

Windows PowerShell 3.0

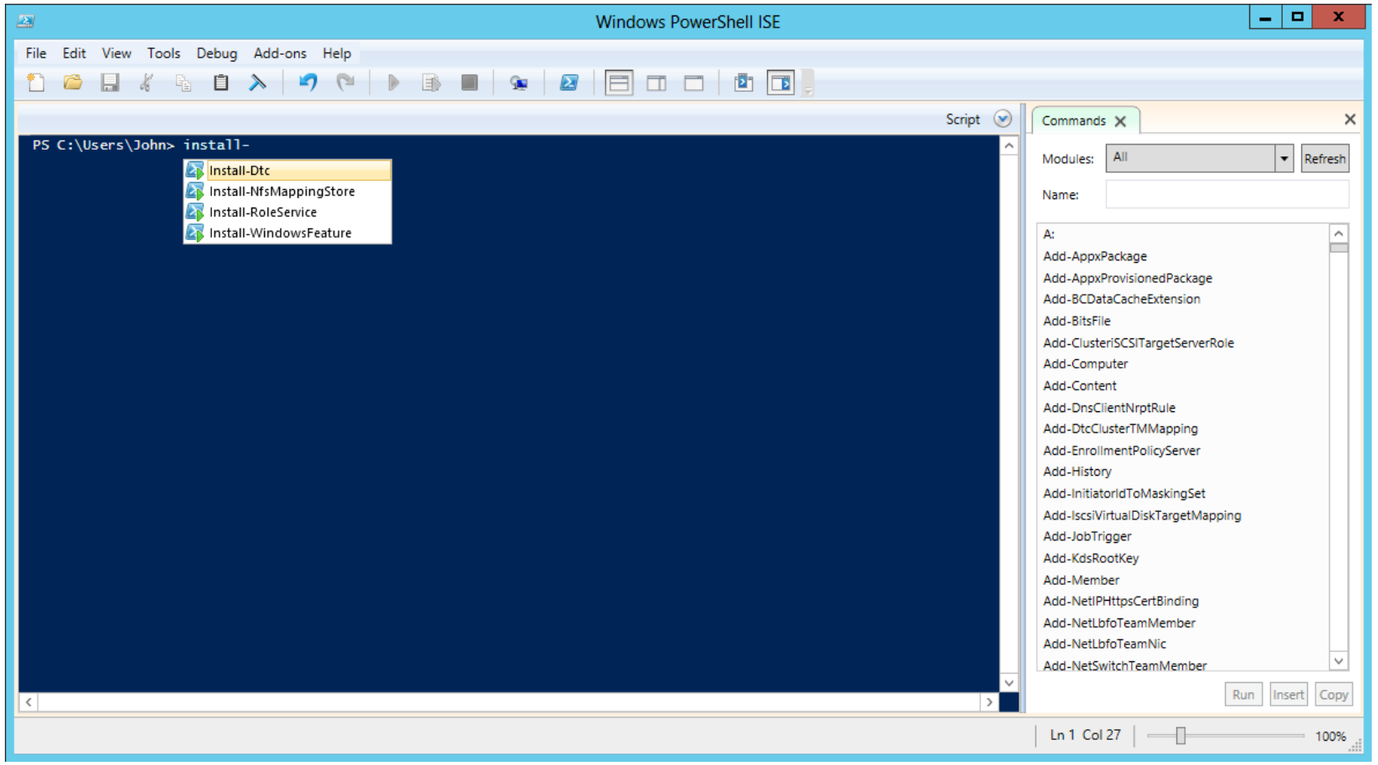
Simplified scripting through Windows PowerShell ISE 3.0

Show-Command pane lets users find and run cmdlets in a dialog box

IntelliSense provides context-sensitive command completion for cmdlet and script names, parameter names and enumerated values, and property and method names



Make sure PowerShell is you best friend



- PowerShell 3.0 with over 2000 cmdlets
  - Allows creation scripts with workflow
  - AD PowerShell history helps you get started
  - Newest help files download on demand – *Update-Help*

Optimized platform based on Server Core

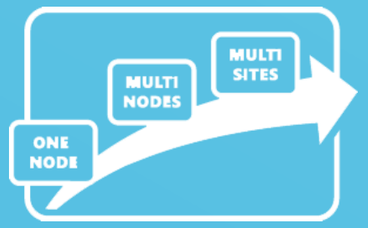
Dynamic Footprint

Minimizing size and security attack surfaces at all times

- **Dynamic remotely managed Servers:** All Servers can be remotely managed and deployed as Server Core with all critical roles as well as on-demand feature management
- **Flexibility at all times**: Choose between Server Core (the default) or Full Server or run without the shell with no re-install
- **Features on Demand:** Use and install exactly the capabilities you need, nothing more
- **Reduced disk size:** Install from a remote repository on your network and not in every image

Windows Remote Management (WinRM) is on by default

Secure Remote Management



Standards based protocol and capabilities for management and workflows

- **Robust Sessions:** PowerShell remote sessions can be re-established and managed by users on multiple machines
- **Integrated DoS protection**: WinRM provides a fixed-limit queue for access requests, prior to their authentication
- **Trusted connections**: Once an administrator has successfully connected their address details are stored to ensure successful connections when attacks occur

Minimized downtime and maximum uptime

Cluster Based Availability

Cluster-Aware Updating and Integrated Encryption

- **Automatic updates:** Patch every node in a cluster with no application downtime
- **Integrated cluster automation:** Transparently takes each node offline by pausing, draining and fallback to apply all updates
- **BitLocker enabled clusters**: AD Cryptography Next Generation used to enable encrypted Cluster Shared Volumes for physical security

Granular authorization policies

Enhanced Data Security and Compliance

Offers granular access to data and corporate resources based on strong identity and device security status, as well as simplified configuration and administration for remote access

- **Central access policies and authorization**: Define who can access what information within the organization based on claims and dynamic policies
- **Active Directory Federation Services**: Integrates Active Directory claims with AD FS allowing the claims from Kerberos tickets to be transformed into SAML tokens for use with claims aware applications both inside the corporate network and across federated trusts
- **Audit policies for compliance reporting**: Identify who accessed highly sensitive information

Policy and delegation enhancements

Finer-grain Security Controls

Allows administrators to more easily and accurately express their intentions around password-policy and delegation of the right to act on behalf of other users in n-tier application scenarios

- **Fine-Grained Password Policy**: Active Directory Administrative Center simplifies the creation and administration of fine-grained password-policies (policies that can be configured to impose different constraints and assigned more granularly than their domain-policy counterparts)
- **Kerberos Constrained Delegation (KCD)**: Extends KCD functionality to cross-domain and cross-forest scenarios while also shifting this important administrative decision to the resource owners rather than the domain administrator

Simplifying Active Directory

Simplified Identity Management

Active Directory provides simplicity and flexibility for the hybrid environment

- **Virtualizing Active Directory**: Domain controller cloning provides elastic-deployment while virtualization safeguards ensure service continuity
- **Simplified Management**: Integrated object-deletion recovery and automatic PowerShell script-generation simplify disaster recovery and automation of important identity management tasks
- **Group Managed Service Accounts**: Windows services running across multiple machines share a single user account with automatic password management

Avoiding Data Leakage

More flexible deployment

Stronger cryptography

0101100010111010
1101111100100010
1011000010111010
0100101011011100

Easier Management

Active Directory Rights Management Services provides enhanced deployment flexibility in Windows 8, with more cryptographic options, remote deployment, support for Server Core, enhanced remote management and more.

DNS Security Extensions

Windows 2012 enhances DNS Security (DNSSEC) with dynamic updates, improved encryption and integrated key management with AD

- **Supports the latest DNS Security standards:** NSEC3 plus RSA/SHA-2 encryption
- **DNS Dynamic Updates**: DNS zone can be signed online, with DNS dynamic updates now enabled
- **AD Integration**: Uses Active Directory to store and distribute keys used for DNS record signing, with automatic rollover support

Information Protection Scenarios

Windows 2012 enhances existing information protection scenarios and supports new ones

- **Simple delegation**: Support employees that need to delegate email management to an assistant
- **Enhanced File Classification integration**: Active Directory Rights Management Services now integrates with file servers out of the box to automatically detect, classify and protect documents based on content and context

Take control of your PKI

Certificate Services Deployment

Easier deployment

New key management options

Enhanced template management

Active Directory Certificate Services now supports TPM-protected keys, enhanced key management, more flexible deployment and configuration tools and a powerful template management user interface.

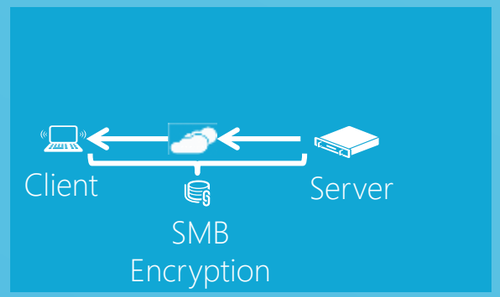
Enhanced Certificate Management

Reduced certificate failures and manual labor

- **Certificate Lifecycle Notifications**: Flexible notification types based on policy to reduce errors and outages
- **Key Based Auto-Renewal:** Support for offline enrollment and subsequent automatic renewal
- **Group Protected PFX**: The password included in the PFX is limited to a set of SIDs using new data protection APIs

Simplified protocol encryption

SMB Encryption



Protecting data from attack on shared or untrusted networks

- **Simple deployment**: End-to-end encryption of SMB data in flight with no new infrastructure or specialized hardware
- **Flexible configuration:** Defined on a per share basis or for the entire server
- **Secure multi-tenancy:** Enables a variety of scenarios where data traverses untrusted networks or WANs

Every App, Any Cloud

Scalable and Elastic Web Platform

Improves web site density, elasticity, and efficiency, while enabling service providers to better build, provision, and manage a hosting environment

- **Scalability and Management**: Scale up using next-generation hardware, NUMA support and CPU Throttling for maximum performance
- **Centralized SSL Certificate Support**: Rapidly add servers to a web farm without manually configuring SSL; centrally share and manage SSL certificates
- **Flexible tools and extensions**: Open source software support using common tools, languages and capabilities

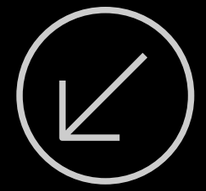
Continued investment in secure software

Security Development Lifecycle

Tools to support all phases of development from requirements to release

- **Holistic and comprehensive approach**: Integration with Visual Studio Team System
- **Improved threat modeling**: Design reviews and requirements validation performed early
- **More and stronger fuzzing tools**: Additional tools including FxCop, Binscope, AppVerifier and Attack Surface Analyzer
- **Public tools and guidance**: All available for download from the Microsoft SDL Portal

Microsoft TechEd 2012



Disaster Recovery

Disaster Recovery Challenges

- Cost
- Complexity
- Inflexibility
- Initial Replication
- Distance Requirements

Hyper-V Replica
Unlimited Replication

- Disaster Recovery Scenarios:
  - Planned, Unplanned and Test Failover
  - Pre-configuration for IP settings for primary/remote location
- Key Features:
  - RPO/RTO in minutes
  - Seamless integration with Hyper-V and Clustering
  - Automatically handles all VM mobility scenarios (e.g. Live migration)
  - Supports heterogonous storage between primary and recovery
  - Integrates with Volume Shadow Services (VSS)

Hyper-V Replica

Complements Array Based Replication

	Replication Provider	Cost	Management	Performance
Hyper-V Replica	Microsoft	• Flexible Storage Options Available • Unlimited VM Replication included	• VM Granularity • Open APIs provide extensibility, interoperability and prevent vendor lock-in	• 5 minutes RPOs • Application Level Consistency • File Level Consistency
Storage Based Replication	NetApp, HP, Fujitsu, IBM, Hitachi, FalconStor, 3Par, EMC, LSI, Compellent, EqualLogic and more…	• High end replicating storage • Additional replication software	• LUN-VM Layout • Coordination with storage team	• Synchronous Replication • High Data Volumes

References

- Windows Server 2012 site:
  - http://www.microsoft.com/windowsserver
  - Including the Windows Server 2012 Datasheet
- Microsoft Security Development Lifecycle Portal:
  - http://www.microsoft.com/security/sdl/default.aspx

CDIC2013

Cyber Defense Initiative Conference

" THE PIRATES IN CYBERSPACE "

โครงการอบรมการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 12

- CDIC 2013 Key Highlights
- CDIC for Management
- CDIC for IT Professional
- CDIC for Amateur
- CDIC Conference Workshop

Advanced Mobile Application Attack and Defense

- *Mobile Application Vulnerability (SSLstrip and OWASP Top 10)*
- *Mobile App Exploit (Mercury)*

Cloud Forensics

- *Cloud Application Forensics Computer Platform*
- *Cloud Application Forensics Smartphone Platform*
- *Free Mail Forensic – Cloud Storage Forensics*

CDIC 2013 Live Show !!

- *Wireless WPA2 PEAP*
- *WPS Brute-Force*
- *Wifi Pineapple- HotSpot Pen-Testing*
- *Evilgrade – Blindly Exploitation*
- *Firefox XPI Exploit*
- *HTML5 Hacking*
- *HiperText Access Exploit*
- *Pivot and Forward Tunnel*
- *Mobile App Malware*
- *FlashBack Trojan for Mac User*

CDIC2013

Cyber Defense Initiative Conference

" THE PIRATES IN CYBERSPACE "

โครงการอบรมการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 12

CDIC 2013 Key Highlights

- *Update Top Ten Threats and Trends on IT & Information Security in 2013 and Beyond*
- *Int'l Conference, IIA, RSA 2012-1023 Highlights*
- *National Cybersecurity Master Plan and Strategies vs. ASEAN ICT Master Plan and Strategies*
- *Business - Organizational Resilience - the Next Step Forward for Business Continuity*
- *Evaluating and Managing Cyber Risks & Security Impacting an Organization*
- *Actions on Threat Horizon 2013*
- *Security Insights on Threat Horizon 2014*
- *How to Upgrade COBIT 4.1 with new COBIT 5*
- *How to Upgrade New ISO/IEC 27001*
- *GRC Security Approaches and Roadmap*
- *Unified Compliance and Security Standards*
- *IT Consumerization and BYOD Policy*
- *How to Secure Online and Internet Banking from Reforming Man-in-the-Middle Attacks*
- *Online Privacy Threats & Behavioral Social Networking Security*
- *Lessons Learned and Truths about Cloud Security and Services*
- *Mobile Malware Transformation*
- *Advanced Botnet-based Distributed Denial of Service (DDoS)*
- *Real Case Studies from the Professionals and Experts*
- *In-depth Live Show Demonstration on New Advanced Cybercrime and Ethical Hacking Techniques*

www.cdicconference.com

CDIC 2013 conference,
27-28 February @Central World
Bangkok, Thailand

www.acisonline.net

ACIS Professional Center Co., Ltd.

www.TISA.or.th

Thailand Information Security Association,

Email : prinya@acisonline.net

Facebook : www.facebook.com/prinyah

Twitter: www.twitter.com/prinyaACIS

Thank You ☺